ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САМАРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ имени академика С. П. КОРОЛЕВА» (САМАРСКИЙ УНИВЕРСИТЕТ)

ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ СРЕДСТВ АСИММЕТРИЧНОЙ КРИПТОГРАФИИ

Самара 2017

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САМАРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ имени академика С.П. КОРОЛЕВА»
(САМАРСКИЙ УНИВЕРСИТЕТ)

ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ СРЕДСТВ АСИММЕТРИЧНОЙ КРИПТОГРАФИИ

Составитель К.Е. Климентьев

Самара
Издательство Самарского университета
2017

УДК 004.056.55
ББК 32.972

Составитель ***К.Е.Климентьев***

Рецензент: к.т.н., доцент А.В.Баландин

Практическое применение средств асимметричной криптографии: [Электронный ресурс]: метод. указания / сост. *К.Е. Климентьев*. - Самара: Изд-во Самарского университета, 2017. – 14 с. : ил. Электрон. текстовые и граф. дан. (Кбайт).- 1 эл. опт. диск (CD-ROM).

Предназначены для студентов, изучающих в рамках направления подготовки 09.03.01 «Информатика и вычислительная техника» курс «Защита информации» и прочие курсы аналогичной тематики.

Содержат необходимый теоретический и справочный материал для выполнения лабораторных работ. Также могут быть использованы в курсовом и дипломном проектировании.

Подготовлены на кафедре информационных систем и технологий.

УДК 004.056.55
ББК 32.972

Оглавление

Введение

Криптография - наука о шифровании данных. Также предметом изучения современной криптографии служат методы обеспечения и проверки подлинности сообщений.

Ц_е_л_ь л_а_б_о_р_а_т_о_р_н_о_й р_а_б_о_т_ы: изучение криптографических методов, основанных на «асимметричных» шифрах (см. ниже).

Задание на лабораторную работу

1. Ознакомиться с принципами современной криптографии (см. п. 1). Особое внимание уделить п.1.4 «Применение асимметричной криптографии».
2. Создать на носителе компьютера два каталога (папки, директории), в каждый из которых поместить отдельный экземпляр программы PGP/GnuPG. (Для запуска MS-DOS-версий воспользоваться средствами виртуальной машины DosBox).
3. Средствами программы PGP/GnuPG смоделировать взаимодействие двух абонентов (Алисы и Боба) в двух ситуациях: 1) обмен приватными сообщениями в рамках схемы «Шифрование с открытым ключом» (см. п. 1.4.1); 2) генерация и проверка электронно-цифровой подписи (см. п. 1.4.2).
4. Записать использованные команды PGP/GnuPG и продемонстрировать процесс моделирования преподавателю.

1. Принципы современной криптографии

1.1. Современные шифры

Зашифрование - обратимое преобразование данных в форму, не пригодную для непосредственного восприятия и использования.

Расшифрование – операция, обратная к шифрованию.

Шифр – какая-либо система алгоритмов и правил, описывающая соответствующие друг другу процедуры зашифрования и расшифрования.

Ключ шифра – секретный параметр, без знания которого невозможно ни зашифрование, ни расшифрование. В современных шифрах ключ – целое число, причем настолько большое, что его невозможно подобрать в разумные сроки (например, 100 двоичных или 30 десятичных цифр).

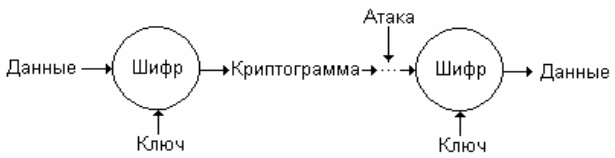

Рис. 1. Принцип использования шифров

Криптостойкость шифра – способность шифра противостоять определению ключа по зашифрованным данным или расшифрованию данных вообще без знания ключа.

Принцип Керкгоффса (сформулирован в XIX в.) – криптостойкость шифра должна зависеть только от секретности ключа, а алгоритмы зашифрования и расшифрования могут быть общедоступными.

Классификация современных шифров изображена на рис. 2.

Рис. 2. Классификация современных шифров

Симметричные шифры требуют для зашифрования и расшифровывания один и тот же ключ.

Потоковые симметричные шифры (см. табл. 1) работают с потоком входных данных и позволяют сразу зашифровывать каждый вновь появляющийся элемент (например, бит) входных данных.

Таблица 1 – Некоторые симметричные потоковые шифры

Шифр	**Длина ключа**	**Примечание**
RC4	8÷512	Применяется для шифрования трафика в Интернете
A5	64	Применяется для шифрования трафика сотовой связи
Однора-зовый блокнот	Длина равна длине набора данных	Абсолютно стоек, применяется в дипломатии для обмена особо важными данными

Блочные симметричные шифры (см. табл. 2) требуют предварительного разбиения входного потока данных на блоки, каждый из которых зашифровывается независимо от других.

Таблица 2 - Некоторые симметричные блочные шифры

Шифр	**Длина блока**	**Длина ключа**	**Примечание**
DES	64	56	Старый национальный стандарт США
3DES	64	3×56=168	Тройной DES: $Y=DES_{K1}(DES_{K2}(DES_{K3}(X)))$
DESX	64	3×56=168	DES + XOR: $Y=K1 \oplus DES_{K2}(X \oplus K3)$
AES	128, 192, 256	128, 192, 256	Новый национальный стандарт США
Skipjack	64	80	Встроен в чипы Fotrezza и Clipper, США
Магма	64	256	ГОСТ 28147-89 и ГОСТ Р 34.12-2015

Окончание табл. 2

Кузнечик	128	256	ГОСТ Р 34.12-2015
IDEA	128	128	Не запатентован
CAST	64, 128	128, 256	Не запатентован
Blowfish	128	64÷448	Опубликован в книге Б. Шнейера
TEA	64	128	Не запатентован, очень компактен
Калина	128,196,256,512	128,196,256,512	Стандарт ДСТУ 7624:2014, Украина
Belt	128	256	Стандарт СТБ 34.101.31-2011, Беларусь
Camellia	128	128,196,256	Стандарт Японии
SM4	128	128	Стандарт КНР
Serpent	128	128, 192, 256	Финалист конкурса «AES»

Предельная длина ключа симметричного шифра, доступного для полного перебора вариантов, на текущий момент составляет 80-90 битов.

Основной недостаток симметричных шифров – сложность распространения общего ключа *K*.

1.2. Современные хеш-функции

Хеш-функция (синонимы - «*функция цифровой свертки*», «цифровой дайджест») - система алгоритмов и правил, описывающая однозначное отображение *прообраза* (произвольного набора данных произвольной длины) в *образ* (в значение фиксированной длины, например, в число, строку и т.п.) – см. рис. 3.

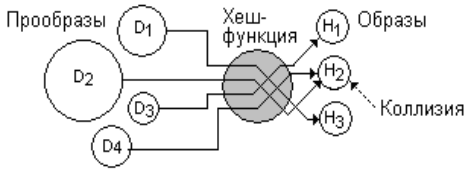

Рис. 3. Хеш-функции

Хеш-функция с ключом – хеш-функция, значение которой не может быть вычислено без знания секретного ключа. Алгоритм таких хеш-функций основан на том или ином шифре.

Если два произвольных набора данных отображаются на различные значения хеш-функций, то эти наборы данных так же различны.

Если два произвольных набора данных отображаются на одно и то же значение хеш-функции, то с очень высокой степенью вероятности эти наборы данных совпадают. Редкая ситуация, когда это правило не выполняется, называется *коллизией* (см. рис. 3).

Полезные свойства хеш-функций:

- необратимость – сложность определения прообраза по образу;
- устойчивость к коллизиям – сложность генерации коллизий.

Таблица 3 – Некоторые хеш-функции

Хеш	**Длина**	**Примечание**
CRC	8, 12, 16, 32	Легко обратима, широко используется в технике
MD5	160	Популярна, недостаточно устойчива к коллизиям
Семейство SHA	256, 384, 512	Используются в Интернете
ГОСТ Р 34.11-94	256	Требует ключа, основана на шифре ГОСТ 28147-89
Keccak (SHA-3)	224, 256, 384, 512	Используется в Интернете

1.3. Асимметричная криптография

Асимметричные шифры (см. табл. 4) используют для зашифрования и расшифрования разные ключи K_E и K_D.

Точнее, K_E и K_D представляют собой две «половинки» одного общего ключа K. Обычно одна «половинка» пары объявляется открытой (общедоступной, публичной), а другая является секретной (приватной). Важно, что по одной «половинке» определить другую практически невозможно.

Цифровой сертификат – электронный документ, содержащий «половинку» ключа асимметричного шифра, а так же вспомогательную информацию: идентификатор хозяина ключа, предельный срок действия ключа, контрольную сумму и прочее. Цифровые сертификаты могут быть встроены в операционные системы и прикладные программы, содержаться в

специальных общедоступных базах данных (репозиториях), храниться на специальных носителях («токенах» безопасности) и т.п.

Таблица 4 – Некоторые асимметричные шифры

Шифр	**Длина ключа**	**Примечание**
RSA	256÷4096	Основан на сложности факторизации целых чисел
El-Gamal	256÷4096	Основан на сложности дискретного логарифмирования
«Эллиптические» шифры	256÷4096	Основаны на сложности решения вычислительных задач в поле корней эллиптических уравнений

Предельная длина ключа асимметричного шифра, доступного для направленного перебора вариантов, может быть охарактеризована результатами открытого международного конкурса RSA Challenge (см. табл. 5).

Таблица 5 - Промежуточные результаты конкурса «RSA Challenge»

Дата взлома	**Длина ключа**	**Техника**	**Сроки взлома**
Февраль 1999 г.	140 цифр, 463 бита	185 компьютеров	1 месяц
Август 1999 г.	155 цифр, 512 битов	292 компьютера	15 недель
Апрель 2003 г.	160 цифр, 530 битов		
Декабрь 2003 г.	174 цифры, 576 битов		
Ноябрь 2005 г.	193 цифры, 640 битов	30 компьютеров	5 месяцев
Май 2005 г.	200 цифр, 663 бита	80 процессоров	3 месяца
Сентябрь 2013	210 цифр, 696 битов		
Июль 2012 г.	212 цифр, 704 битов		
Май 2016 г.	220 цифр, 729 битов		
Декабрь 2009 г.	232 цифры, 768 битов		

В настоящее время практическое применение ключей длиной менее 1024 битов считается небезопасным. Рекомендуемая длина – 2048 битов.

1.4. Применение асимметричной криптографии

Пусть X - исходные данные, подлежащие зашифрованию с ключом K_E, а Y - зашифрованные данные (криптограмма), которые могут быть расшифрованы ключом K_D (см. рис. 4).

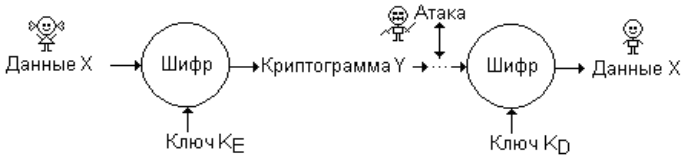

Рис. 4. Модель канала связи

Предположим, что два абонента - Алиса и Боб - собираются обмениваться секретной информацией по открытому каналу. Злодей имеет возможность прослушивать этот канал.

1.4.1. Шифрование с открытым ключом

1. Боб генерирует ключевую пару $K=(K_E,K_D)$.

2. Боб объявляет ключ K_E открытым и публикует его (то есть раздает всем желающим по открытому каналу – см. рис. 5). Теперь обладателями ключа

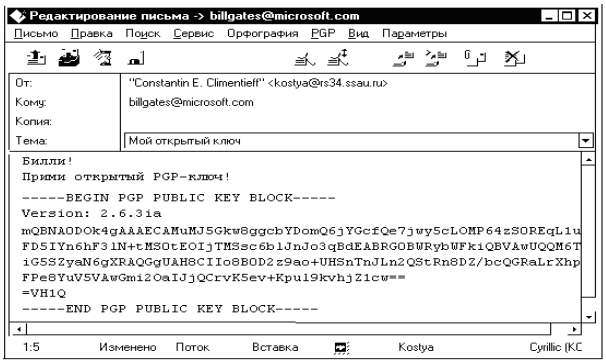

Рис. 5. Публикация открытого ключа письмом электронной почты

K_E являются и Алиса, и Злодей. Но ни Алиса, ни Злодей не могут по «половинке» K_E определить секретную «половинку» K_D.

3. Алиса формирует приватное сообщение X, шифрует его ключом K_E и передает Бобу криптограмму Y по открытому каналу. Злодей может перехватить криптограмму Y, но не способен ее расшифровать, потому что не имеет расшифровывающего ключа K_D.

4. Единственный человек в мире, который может расшифровать криптограмму Y и прочитать сообщение X это Боб, потому что только он владеет расшифровывающим ключом K_D.

Это схема *шифрования с открытым ключом*. Практическое использование ее заключается в следующем.

1. Обмен приватными сообщениями по электронной почте. Средства автоматического зашифрования и расшифрования электронных писем асимметричным шифром RSA встроены в отечественный почтовый клиент TheBAT (см. рис. 5).

2. Обмен приватными *сеансовыми* (одноразовыми) ключами, которые в дальнейшем используются для шифрования Интернет-трафика при помощи быстрых потоковых или блочных шифров. Таким образом нейтрализуется основной недостаток, свойственный симметричным шифрам (см. п. 1.1).

П_р_и_м_е_ч_а_н_и_е. Поскольку операция шифрования больших объемов данных асимметричным шифром очень медленна, на практике применяется следующая схема. Сначала генерируется короткий *сеансовый* (одноразовый) ключ для какого-нибудь «быстрого» шифра (например, AES с ключом 128 битов – см. табл. 2 в п.1.1) и данные шифруются именно этим шифром с именно этим сеансовым ключом. Затем короткий сеансовый ключ шифруется асимметричным шифром с помощью постоянного мастер-ключа K_E и передается вместе с криптограммой. Расшифрование производится в обратном порядке.

1.4.2. Электронная цифровая подпись (ЭЦП)

1. Алиса генерирует ключевую пару $K=(K_E,K_D)$.

2. Алиса объявляет ключ K_D открытым и публикует его (то есть раздает всем желающим по открытому каналу). Теперь обладателями ключа K_D являются и Боб, и Злодей. Но ни Боб, ни Злодей не могут по «половинке» K_D определить секретную «половинку» K_E.

3. Алиса формирует сообщение X, шифрует его секретным ключом K_E и передает Бобу криптограмму Y по открытому каналу.

4. Боб может расшифровать криптограмму Y и прочитать сообщение X, поскольку обладает «половинкой» K_D. Злодей так же может сделать это, но он

не способен подделать сообщение, поскольку не обладает шифрующей «половинкой» K_E.

5. Таким образом, никто в мире не может подделать сообщение X, сформированное Алисой. С другой стороны, Алиса не может отказаться от авторства сообщения X.

Это схема *электронной цифровой подписи* (синонимы – *цифровая подпись*, *электронная подпись*).

П_р_и_м_е_ч_а_н_и_е. Поскольку операция шифрования больших объемов данных асимметричным шифром очень медленна, на практике применяется следующая схема формирования ЭЦП. Для подписываемого набора данных рассчитывается короткое значение хеш-функции (например, MD5 всего 160 бит – см. п.1.2 и табл. 3), которое подвергается шифрованию с ключом K_E и «прикладывается» к открытому набору данных. При проверке подлинности сообщения ключом K_D расшифровывается значение хеш-функции, «приложенное» к данным, и сравнивается со значением хеш-функции, рассчитанным по данным самостоятельно. При совпадении подлинность и целостность данных считаются доказанными.

Применение электронно-цифровой подписи.

1. Подписание электронных документов (в том числе финансовых). Проверка подлинности документа выполняется путем расшифрования открытым ключом K_D, хранящимся в общедоступных репозиториях. Такие ключи K_D официально привязываются к конкретному физическому или юридическому лицу и называются «*квалифицированными*». Любое юридическое или физическое лицо может получить и зарегистрировать свой ключ K_D (точнее, цифровой сертификат с ключом K_D) в специальном *сертификационном центре*.

2. Проверка подлинности программного обеспечения, подписанного производителем при помощи секретного ключа K_E, выполняется в процессе инсталляции операционной системой, в которую «встроен» открытый ключ K_D.

2. Использование программы PGP

Во многих странах (в том числе, в РФ и США) изготовление, обслуживание, коммерческое использование и распространение средств криптографии законодательно ограничены. Так же многие шифры и хеш-функции запатентованы и для своего использования требуют получения лицензии от правообладателя.

OpenPGP – открытый международный стандарт на некоммерческие криптографические средства. Он описывает алгоритмы «бесплатных» шифров и хеш-функций, форматы организации данных, методы генерации и распространения ключей, способы создания и проверки электронно-цифровых подписей и т.п. Криптографические средства, удовлетворяющие этому стандарту, в значительной степени совместимы друг с другом.

PGP (англ. Pretty Good Privacy – Вполне Хорошая Приватность) – программа шифрования данных и работы с ЭЦП, удовлетворяющая стандарту

OpenPGP. (Точнее, возможности и особенности ранних версий этой программы послужили основой для OpenPGP). Ранние консольные версии для MS-DOS и Unix, созданные в 1990-х годах Ф.Циммерманом (США), бесплатны. Начиная с 2000-х годов версии для Windows и иных операционных систем, разрабатываемые в Symantec Corp. (США), являются коммерческим продуктом. Однако «коммерческие» и «некоммерческие» версии в значительной степени совместимы по форматам ключей, способам хранения данных и т.п.

GNUPg – бесплатная программа, удовлетворяющая стандарту OpenPGP. Внешне идентична ранним версиям программы PGP и совместима с ними, хотя существуют версии не только для MS-DOS, но и 32-битовые и 64-битовые консольные версии для Windows, для Linux и иных операционных систем. Поддерживает пользовательский интерфейс на многих языках, в том числе и на русском.

2.1. Методика применения

Основное назначение программ PGP/GNUPg – шифрование и электронно-цифровое подписание сообщений электронной почты в соответствии с принципами асимметричной криптографии (см. п. 1.4).

Для использования программы PGP каждому пользователю необходимо иметь, как минимум, пару ключей (K_E,K_D). Как правило, эти ключи однократно генерируются пользователем при помощи какой-нибудь из версий программы PGP/GHUPg, а затем многократно и долговременно используются им в самых разных обстоятельствах.

Каждый из ключей может быть представлен в нескольких различных форматах.

Формат 1 – текстовый. Он удобен для передачи открытых ключей другим лицам в виде документа, электронного письма и т.п., например:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia
mQBNA0DOk4gAAAECAMuMJ5Gkw8ggcbYDomQ6jYGcfQe7jwy5cLOMP64zS0REqL1u
...
FPe8YuV5VAwGmi2OaIJjQCrvK5ev+Kpul9kvhjZ1cw==
=VH1Q
-----END PGP PUBLIC KEY BLOCK-----
```

Формат 2 – двоичный цифровой сертификат. Такой вид ключа обеспечивает целостность и подлинность ключа, он удобен для операций над ключами – для встраивания в почтовые программы, для переноса из одной версии PGP в другую и т.п.

Формат 3 – элемент базы данных. Программа PGP ведет две внутренних базы данных:

- pubring - для хранения публичных ключей пользователя и других лиц;
- secring – для хранения секретных ключей пользователя.

Поскольку программой PGG/GNUPg могут пользоваться разные пользователи, каждый ключ в базе данных ассоциирован с конкретным пользователем. Для выполнения операций над ключом (создание, удаление,

экспорт из базы данных, импорт в базу данных, зашифрование, проверка ЭЦП и пр.) каждый раз запрашиваются логин и пароль конкретного пользователя.

2.1.1. Работа с ключами

1. Сгенерировать новую ключевую пару можно командой **pgp –kg**. В процессе генерации пользователю потребуется:

1) выбрать «RSA key size» - размер ключа в битах (в рамках лабораторной работы достаточно 256, на практике – не менее 1024);
2) выбрать «user ID» - уникальный идентификатор, который будет однозначно соответствовать ключевой паре;
3) выбрать и два раза ввести «pass phrase» - пароль, по которому пользователь будет получать доступ к ключам, хранящимся в базе данных;
4) нажать требуемое число раз на произвольные клавиши в произвольные моменты времени, чтобы позволить программе сгенерировать истинно случайное число.

Сгенерированные ключи автоматически будут помещены в базы данных.

2. Просмотреть содержимое базы данных можно командой **pgp –kv [userid] [keyring].**

Если не указан конкретный userid (идентификатор пользователя), то будут показаны все ключи, хранящиеся в базе данных. Если не указано имя базы данных, то по умолчанию будет просмотрено содержимое базы открытых ключей «pubring.pgp». Если ключи хранятся в нестандартной базе данных, то можно воспользоваться командой **pgp keyname** без дополнительных ключей.

3. Добавить новые ключи из сертификата keyname в базу данных keyring можно командой **pgp –ka keyname [keyring].**

4. Удалить определенный ключ с идентификатором userid из базы данных keyring можно командой **pgp –kr userid [keyring].**

5. Экспортировать определенный ключ с идентификатором userid в файл сертификата keyfile можно командой **pgp –kx userid keyfile [keyring].**

7. Экспортировать определенный ключ с идентификатором userid в текстовый файл keyfile можно командой **pgp –kxa userid keyfile [keyring].**

2.1.2. Работа с данными

В программе PGP шифрование данных (предварительно сжатых методом ZIP) выполняется симметричным блочным шифром со случайным сеансовым ключом по технологии, описанной в п.1.4.1. Данные зашифровываются шифром IDEA (см. табл. 2) с одноразовым сеансовым ключом, потом этот ключ шифруется ключ методом RSA (см. табл. 4) с мастер-ключом keyname.

1. Зашифровать текстовый файл textfile при помощи открытого ключа с идентификатором her_userid можно командой **pgp -e textfile her_userid**. Также можно указать список идентификаторов, разделяя их пробелами, например: **pgp file.txt sasha masha misha natasha**, в этом случае будет получено несколько копий исходного файла, зашифрованных с разными ключами.

2. Расшифровать зашифрованный файл или проверить электронную подпись под ним можно командой **pgp filename**. Если в базах данных содержится нужный ключ, содержимое указанного файла будет расшифровано. Если необходимо указать специальное имя файла, в который будет помещен результат, можно воспользоваться той же командой в форме **pgp filename –o resultname**.

3. Для электронного подписания файла textfile при помощи своего закрытого ключа необходимо ввести команду **pgp –s textfile** (двоичный результат будет помещен в textfile.pgp). Если результат должен остаться в текстовом виде, то необходимо использовать команду **pgp –sta textfile** (текстовый результат будет помещен в textfile.asc). Для подписания текста своим закрытым ключом и шифрования его чужим открытым ключом (с идентификатором her_userid) используется команда **pgp -es textfile her_userid**.

Литература

1. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: Учебный курс. – М.: Горячая линия-Телеком, 2002. – 175 с.

2. Бернет С., Пэйн С. Криптография. Официальное руководство RSA Security. – М.: БИНОМ, 2002. - 384 с.

Методические материалы

ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ СРЕДСТВ АСИММЕТРИЧНОЙ КРИПТОГРАФИИ

Методические указания

Составитель ***Климентьев Константин Евгеньевич***

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САМАРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ имени академика С.П. Королева»
(Самарский университет)
443086, САМАРА, МОСКОВСКОЕ ШОССЕ, 34

Изд-во Самарского университета
443086, Самара, Московское шоссе, 34.